OLLSCOIL NA GAILLIMHE
UNIVERSITY OF GALWAY

Semester 2 Examinations 2022/2023

Course Instance Code(s)	4BCT, 1MECE, 1OA, 1EM
Exam(s)	B.Sc. (Computer Science & Information Technology), M.E. (Electronic and Computer Engineering)
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	1
External Examiner(s)	Dr. Ramona Trestian
Internal Examiner(s)	Prof. Michael Madden *Dr. Michael Schukat

Instructions: **Answer Question 1 and 2 other questions.**

Duration	**2 hours**
No. of Pages	**4**
Discipline(s)	Computer Science
Course Co-ordinator(s)	Dr. Colm O'Riordan

Requirements:

Release in Exam Venue	Yes [X]	No [ ]
MCQ Answersheet	Yes [ ]	No [X]
Handout	None	
Statistical/ Log Tables	None	
Cambridge Tables	None	
Graph Paper	None	
Log Graph Paper	None	
Other Materials	None	
Graphic material in colour	Yes [ ] No [X]	

Question 1 (Compulsory)

Assume you are a member of the FarmEye project team that develops an all-weather IP-enabled (IoT) CCTV camera system to monitor farm buildings and farm yards. The product is aimed to tackle the growing problem of farm theft and farm trespassing. The target market are both farmers and security services.
The camera provides a 24/7 life stream, with an uncompressed RGB still image being sent every second. Data communication is provided via a proprietary radio link to a nearby Internet-enabled base station, so an end-to-end encryption of the captured images between camera and base station is required. However, the computational resources on the camera are limited, therefore none of the standard L2/L3/L4 security protocols can be adopted. Instead you are asked to provide a secure data communication protocol that streams data from a single camera to the base station.

a) Identify concrete possible active and passive attacks by a threat actor on the radio data communication link. Based on these, outline the requirements for a secure communication protocol.

[4 marks]

b) Based on your findings in a) devise a simple protocol message format that allows the streaming of data from the camera to the base station. Justify your design.

[3 marks]

c) Version 1 of the communication protocol uses a private key block cipher, with the key shared between the camera and the base station. Show how a simple algorithm can be implemented via a Feistel cipher.

[5 marks]

d) Determine if your image encryption should be done in EBC mode or in CBC mode. Distinguish between both modes of operation, and justify your decision.

[3 marks]

e) Version 2 of the protocol uses a stream cipher instead of a block cipher. Using an example explain how such a stream cipher based on an LFSR could be implemented, and show how the encoding and decoding process works.

[5 marks]

f) Determine how your protocol would benefit from an additional hash function complementary to either version 1 or version 2, and subsequently update your design. Outline how this extension increases the robustness of your protocol.

[4 marks]

g) In order to simplify key management it is suggested to integrate the Diffie-Hellman key exchange protocol. Using an example, show how a key exchange between the camera and the base station could be accomplished. Further on, comment on the security / robustness of this extension and, using an example, show how a threat actor could compromise the key exchange.

[6 marks]

PTO

Question 2

a) The FarmEye product in Question 1 became a commercial success and will be complemented by other wireless sensors and actuators, e.g. motion detectors, that communicate with the base station. In order to avoid 3rd party products to be integrated, and to streamline key management, the project manager decides to have digital certificates installed on every device. Explain, how such a solution would work.
In your answer, make reference to:

a. X.509 certificates and a suitable certificate structure for FarmEye's devices
b. The purpose of the CA and a suitable CA hierarchy
c. How certificate revocation could be implemented
d. How certificate extensions could be used
e. How the device validation and key generation for secure device-to-access point communication would work.

[8 marks]

b) FarmEye customers would like to have camera timestamps attached to the transmitted images. In order to avoid rolling out a new communication protocol that contains such timestamps, it is proposed to use steganographic techniques to add such data to the transmitted pictures. Outline in detail, how this can be done. You can assume that the timestamp itself follows the normal ASCII format, i.e. YYYY:MM:DD:HH:MM:SS".

[2 marks]

Question 3

a) What are timing attacks, and how can they be avoided? Support your answer by providing an example for a safe and an unsafe implementation of a function of your choice.

[5 marks]

b) You've been asked by the principal of your former secondary school to help her assessing Kerberos as a possible authentication solution for the school IT infrastructure (that includes both desktops/workstations and server resources). In your response, explain in some detail, how Kerberos works, and how it would allow authenticating users and controlling access to the schools' server resources. In your answer also comment on the security/robustness of Kerberos.

[5 marks]

PTO

Question 4

a) Using examples where appropriate, explain the following (TLS-related) terms:

- Forward secrecy
- OCSP Stapling
- Authenticated Encryption with Additional Data (AEAD)

[3 marks]

b) What is meant by port scanning? In your answer, use diagrams to explain 2 scans of your choice. Further on, show how systems can be hardened against such scans.

[4 marks]

c) Using an example explain how a simple substitution cipher can be broken via a letter frequency distribution analysis.

[3 marks]